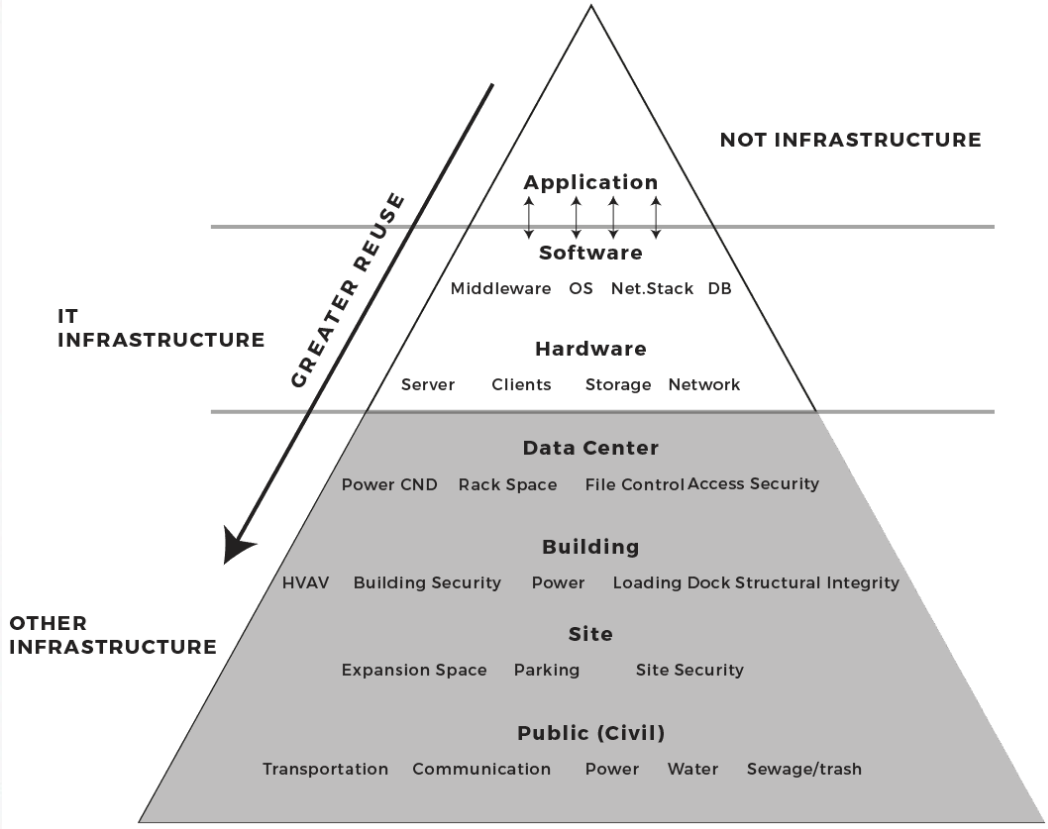
BAB II
LANDASAN TEORI

2.1 Infrastruktur Teknologi Informasi

Menurut (Robertson & Sribar, 2002) definisi dari infrastruktur adalah "*the structure beneath a structure*" dimana hal tersebut memiliki makna suatu struktur atau lapisan dibawah lapisan yang saling mendukung setiap lapisan diatasnya. Dapat pula diaartikan dengan menyediakan suatu layanan atau dukungan agar tercapainya lapisan diatasnya. Seperti pada gambar 2.1:



Gambar 2. 1 Infrastuktur Teknologi Informasi (Robertson & Sribar, 2002)

Dari gambar diatas (Robertson & Sribar, 2002) menjelaskan masing-masing struktur atau lapisan pada *pyramid infrastructure* teknologi informasi tersebut memiliki beberapa karakteristik, diantaranya:

1. Pemakaiannya lebih luas dibanding struktur atau lapisan yang ada di atasnya.

2. Lebih permanen/statis dibanding struktur di atasnya.
3. Terhubung secara fisik dengan struktur di atasnya.
4. Sering dikenal sebagai *support*//layanan pendukung.
5. Terpisah (*distinct*) dari struktur-struktur yang didukungnya dalam hal siklus hidupnya (*plan, build, run change, exit*).
6. Dimiliki dan dikelola oleh pihak yang berbeda dari struktur yang didukungnya.

Gambar 2.1, menjelaskan bahwa infrastrukur teknologi informasi sebagai struktur atau lapisan yang memberikan layanan dan dukungan (*support*) terhadap lapisan yang ada di atasnya. Lapisan *Application* tidak dikatakan sebagai bagian dari infrastruktur karena *Application* merupakan puncak atau hasil akhir dari siklus hidup infrastruktur teknologi informasi.

2.2 Keamanan Informasi

Menurut (Utomo et al., 2012) keamanan informasi merupakan suatu langkah atau upaya yang dilakukan untuk melindungi aset informasi yang dimiliki. Upaya perlindungan tersebut dilakukan dengan tujuan untuk memastikan keberlangsungan bisnis, meminimalkan risiko yang mungkin terjadi dan memaksimalkan keuntungan yang didapat dari investasi dan kesempatan bisnis.

Menurut (Whitman & Mattord, 2010) keamanan informasi merupakan suatu bentuk perlindungan terhadap informasi dan unsur-unsur penting yang ada di dalamnya seperti kerahasiaan, integritas, dan ketersediaan tidak terkecuali sistem dan perangkat keras yang digunakan untuk menyimpan dan mengirimkan informasi tersebut. Tiga unsur penting dari keamanan informasi yaitu:

1. Kerahasiaan (*Confidentiality*)

   Kerahasiaan merupakan unsur yang memastikan informasi hanya dapat diakses oleh pihak yang memiliki wewenang atas akses ke informasi tertentu.
2. Integritas (*Integrity*)

   Integritas merupakan unsur yang memastikan bahwa kualitas, keutuhan, dan kelengkapan data terjaga sesuai dengan keaslian data.
3. Ketersediaan (*Availability*)

Kerahasiaan merupakan unsur yang memastikan bahwa pihak yang memiliki hak akses ke suatu informasi dapat mengakses informasi tersebut dalam bentuk yang dibutuhkan tanpa gangguan atau hambatan.

Sedangkan menurut (Iffano & Riyanarto, 2009) keamanan informasi adalah suatu bentuk penjagaan informasi dari seluruh kemungkinaan ancaman yang akan terjadi dengan tujuan untuk memastikan atau menjamin keberlangsungan suatu bisnis (*business continuity*), meminimalisir risiko bisnis (*reduce business risk*) dan mengoptimalkan pengembalian investasi bisnis. Dapat disimpulkan bahwa keamanan informasi sangat diperlukan untuk melindungi informasi sebagai aset penting dalam organisasi dari segala sesuatu yang dapat mengancam keberlangsungan bisnis suatu organisasi saat ini atau dimasa mendatang.

2.3 Audit Keamanan Informasi

Menurut (Iffano & Riyanarto, 2009) dalam buku "Sistem Manajemen Keamanan Informasi – Berbasis ISO 2001" Audit merupakan bentuk evaluasi atau penilaian terhadap suatu organisasi yang dilakukan oleh pihak atau individu yang kompeten dengan tujuan memastikan bahwa objek yang diaudit telah sesuai dengan standar dan regulasi yang dijadikan acuan. Audit atau penilaian merupakan serangkaian proses yang sistematik, independen dan terdokumentasi untuk menemukan bukti-bukti (audit *evidence*) di lapangan terkait keamanan informasi organisasi untuk selanjutnya di sesuaikan dengan standar yang digunakan dan dievaluasi.

Menurut ISACA dalam (Halim, Tanuwijaya, & Adrian, 2012) Audit keamanan informasi adalah proses atau aktivitas yang sistematik, independen dan terdokumentasi untuk menemukan suatu bukti-bukti (audit *evidence*) yang selanjutnya dievaluasi secara obyektif untuk menentukan apakah tingkat objek yang di audit sudah memenuhi kriteria pemeriksaan (audit) yang ditetapkan. Tujuan dari audit adalah untuk memberikan gambaran kondisi tertentu yang berlangsung di organisasi atau organisasi dan pelaporan mengenai pemenuhan terhadap sekumpulan standar yang terdefinisi.

Menurut (Kemenpora, 2012) Audit keamanan informasi adalah suatu alat atau perangkat dalam menentukan, mendapatkan, dan mengelola setiap *level* keamanan dalam suatu organisasi. Audit keamanan informasi bertujuan untuk meningkatkan *level* keamanan informasi, mencegah rancangan keamanan informasi yang tidak layak, dan mengoptimalkan efisiensi tingkat keamanan, dan proses keamanan informasi itu sendiri di suatu organisasi. Hasil dari audit keamanan informasi adalah tersusunnya dokumen laporan audit yang terkait pada keamanan teknologi informasi yang digunakan di lingkungan organisasi tersebut.

Berdasarkan dari definisi audit keamanan informasi diatas dapat disimpulkan pengertian dari audit keamanan informasi adalah suatu kegiatan atau aktivitas yang bertujuan melakukan *assessment* atau penilaian mengenai keamanan informasi suatu organisasi untuk untuk menemukan bukti-bukti yang selanjutnya dievaluasi menggunakan suatu standar yang ditentukan untuk melihat tingkat kesesuaian keadaan keamanan informasi organisasi saat ini dengan standar yang digunakan sebagai pedoman.

Dalam melakukan audit atau penilain sistem manajemen keamanan informasi terdapat 2 jenis audit yang dapat dilakukan, yaitu: Audit Kepatuhan dan Audit Substansi. Pelaksanaan audit itu sendiri dapat tergantung pada kebutuhan serta tujuan audit itu sendiri. Berikut ini akan dijelaskan jenis-jenis audit dalam mengembangkan Sistem Manajemen Keamanan Informasi:

1. Audit Kepatuhan (*Compliance Audit*)

   Audit Kepatuhan adalah audit SMKI yang dilaksanakan dengan tujuan untuk menegaskan apakah Objektif kontrol, kontrol dan prosedur telah memenuhi hal-hal berikut:

   a) Telah memenuhi persyaratan dan ketentuan yang ditetapkan dalam manual SMKI yang dijadikan acuan.
   b) Telah efektif di implementasikan dan dipelihara dalam lingkungan organisasi atau perusahaan.
   c) Telah berjalan sesuai dengan yang diharapkan sesuai dengan manual SMKI yang dijadikan acuan.

2. Audit Substansi (*Subtantion Audit*)

Audit Substansi adalah audit SMKI yang dilaksanakan dengan tujuan menegaskan apakah hasil dari aktivitas (prosedur atau proses telah dijalankan) telah sesuai dengan yang diharapkan.

Pada penelitian yang penulis lakukan mengenai beberapa permasalahan yang telah dijabarakan pada rumusan masalah diatas audit atau penilaian yang dilakukan pada studi kasus yaitu RSUD Arifin Achmad adalah Audit Kepatuhan (*Compliance Audit*).

2.4 Metode Penilaian Risiko

Proses identifikasi risiko bertujuan untuk memahami seberapa besar dan risiko apa yang akan diterima oleh organisasi atau perusahaan jika informasi yang dikelola mendapatkan ancaman atau gangguan keamanan yang menyebabkan gagalnya penjagaan aspek keamanan informasi.

Menurut (Iffano & Riyanarto, 2009) terdapat beberapa langkah dalam melakukan penilaian risiko yang terdiri dari:

1. Mengidentifikasi aset yang dimiliki oleh organisasi atau perusahaan sesuai dengan ruang lingkup SMKI.
2. Menghitung nilai aset berdasarkan aspek keamanan informasi.
3. Mengidentifikasi ancaman dan kelemahan terhadap aset SI/TI yang ada.
4. Melakukan analisis dampak bisnis jika terjadi kegagalan penjagaan aspek keamanan informasi.

Penjelasan lebih lanjut mengenai langkah-langkah dalam melakukan penilaian risiko akan dijelaskan pada sub bab berikut ini.

2.4.1 Identifikasi Aset

Aset adalah segala sesuatu yang memiliki nilai dan berharga bagi organisasi. Identifikasi aset merupakan langkah awal dalam manajemen risiko. Dengan melakukan identifikasi, organisasi dapat mengetahui aset apa saja yang dimiliki beserta nilainya, sehingga organisasi dapat memberikan perlindungan yang tepat pada aset tersebut. Keluaran dari tahapan ini adalah daftar aset yang berkaitan dengan informasi serta nilai aset yang dimiliki. Adapun nilai aset dapat dihitung

berdasarkan aspek keamanan informasi, yaitu *confidentiality*, *integrity* dan *availability*.

Tabel 2. 1 Contoh tabel indentifikasi aset

Kategori Aset	ID Aset	Nama Aset
Informasi	IN-001	Informasi MOU
Perangkat Keras	HD-001	Server
Perangkat Lunak	SW-001	SIM-RS

Setelah aset infrastruktur SI dan TI yang ada sudah teridentifikasi maka langkah berikutnya adalah melakukan penilaian aset berdasarkan pendekatan tiga aspek keamanan informasi yaitu kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availiability*).

Tabel 2. 2 Penilaian aset SI/TI berdasarkan aspek keamanan informasi

Parameter Penilaian	Kriteria	Keterangan	Nilai
Confidentiality (NC)	*Public*	Aset dapat diakses oleh siapapun	1
	Internal Use Only	Aset dapat diakses oleh orang yang memiliki hak akses saja seperti pegawai EDP (Sekretaris, Bagian Software dan pelaporan, dan Bagian Jaringan dan *Maintanance*).	2
	Private	Aset hanya dapat diakses oleh pegawai yang memang ditugaskan untuk mengelola aset yang bersangkutan.	3
Integrity (NI)	*No Impact*	Ketergantungan dan kehandalan dari aset tidak mempengaruhi proses bisnis organisasi.	1
	Minor Incident	Ketergantungan dan kehandalan dari aset mempunyai pengaruh yang sedang dalam proses bisnis organisasi.	2
	Unacceptable Damage	Gangguan integritas tidak dapat diterima/ditolerir sehingga	3

Parameter Penilaian	Kriteria	Keterangan	Nilai
		mengganggu jalannya proses bisnis.	
Availiability (NA)	*Low/No Availability*	Ketersediaan terhadap aset tidak mempengaruhi jalanya proses bisnis organisasi.	1
	Office Hours Availability	Ketersediaan terhadap aset harus tersedia saat jam kerja.	2
	Very High Availability	Ketersediaan terhadap aset harus selalu tersedia demi jalannya proses bisnis organisasi.	3

Setelah melakukan penilaian aset berdasarkan aspek keamanan informasi yaitu: *Confidentiality*, *Integrity* dan *Availability*, selanjutnya dilakukan perhitungan nilai aset menggunakan persamaan matematis sebagai berikut:

Nilai Aset = NC + NI + NA

Berikut ini contoh perhitungan nilai aset infrastruktur SI dan TI:

Tabel 2. 3 Contoh pehitungan nilai aset

Kategori Aset	ID Aset	Nama Aset	NC	NI	NA	Nilai Aset
Informasi	IN-001	Informasi MOU	3	3	1	7
Perangkat Keras	HD-001	Server	1	2	3	6
Perangkat Lunak	SW-001	SIM-RS	2	2	1	5

2.4.2 Mengidentifikasi Ancaman dan Kelemahan Aset

Setelah masing-masing aset telah diketahui nilai asetnya berdasarkan aspek keamanan informasi, maka langkah berikutnya adalah mengidentifikasi daftar ancaman dan kelemahan yang kemungkinan diterima oleh aset, kemudian aset SI/TI yang telah terindentifikasi ditentukan nilai rerataprobabilitas kemunculan ancaman dan kelemahannya dengan menggunakan rentang nilai sebagai berikut:

Tabel 2. 4 Rentang nilai probabilitas ancaman dan kelemahan (Iffano & Riyanarto, 2009)

No	Probabilitas	Deskripsi	Rerata Probabilitas
1	*Low*	Tidak pernah terjadi	0.1 – 0.3
		Tidak lebih dari satu kali terjadi dalam kurun waktu 1 tahun	
2	*Medium*	Pernah terjadi pada kurun waktu 1 bulan	0.4 – 0.6
3	*High*	Sering terjadi dalam waktu 1 tahun terakhir	0.7 – 1.0
		Memiliki potensi terjadi kembali	

Berdasarkan tabel diatas dapat dilakukan perhitungan nilai ancaman (threat and vulnerable) dari suatu aset infrastruktur SI dan TI dengan rumus:

$$\textbf{Nilai Ancaman (NT)} = \frac{\sum \ Probability\ of\ Occurence}{\sum \ \text{Ancaman}}$$

Keterangan:

$\sum$ PO: Jumlah *Probability of Occurence*

$\sum$ Ancaman: Jumlah ancaman terhadap informasi

Berikut ini contoh perhitungan nilai ancaman (*threat* and *vulnerable*):

Tabel 2. 5 Contoh pehitungan nilai aset

ID Aset: HD-001				
Nama Aset: Server Data Center				
Kejadian		**Jenis**	**Probabilitas**	**Rerata Probabilitas**
Kode	**Keterangan**			
T1	Akses tidak sah	Ancaman	*Low*	0.0
T2	Serangan virus	Ancaman	*Low*	0.0
V1	Kesalahan SDM	Kelemahan	*Low*	0.1
V2	Gangguan perangkat keras	Kelemahan	*Low*	0.1

Total Kejadian	**4**	**Jumlah Rerata Probabilitas**	**0.2**
Nilai Ancaman (NT)			**0.05**

Dari contoh data pada tabel diatas dapat dihitung nilai ancaman (NT) terhadap infrastruktur SI dan TI:

$$\textbf{Nilai Ancaman (NT)} = \frac{0.2}{4} = 0.5$$

2.4.3 Analisis Dampak Risiko Bisnis

Analisis dampak bisnis dilakukan untuk mengambarkan tingkat ketahanan proses bisnis yang dijalankan RSUD Arifin Achmad saat aset yang dimiliki terganggu akibat faktor ancaman dan kelemahan yang telah dianalisis. Nilai BIA dibuat untuk mengetahui batas toleransi dari aset yang ada terhadap ancaman dan kelemahan yang muncul. Kriteria penilaian untuk BIA dapat dilihat pada tabel 2.6.

Tabel 2. 6 Kriteria BIA (Utomo et al., 2012)

No	Batas Toleransi	Keterangan	Nilai BIA
1	< dari 1 Minggu	*Not critical*	0
2	1 hari s/d 2 hari	*Minor critical*	1
3	< 1 hari	*Mayor critical*	2
4	< 12 jam	*High critical*	3
5	< jam	*Very high critical*	4

Dengan menggunakan nilai kriteria BIA yang sudah ditentukan maka tahap selanjutnya adalah membuat daftar dampak yang ditimbulkan terhadap aset-aset yang dimiliki RSUD Arifin Achmad yang dapat dilihat pada tabel 2.7.

Tabel 2. 7 Contoh nilai BIA untuk masing-masing aset

No	Aset SI/TI	Batas Toleransi	Dampak yang ditimbulkan	Nilai BIA
1	Informasi MOU	< 1 jam	Tidak memiliki bukti konkrit terkait kerjasama dengan pihak eksternal sehingga	4

No	Aset SI/TI	Batas Toleransi	Dampak yang ditimbulkan	Nilai BIA
			menimbulkan indikasi penyalah gunaan wewenang. Informasi yang dibutuhkan terpending.	
2	Server	< 1 jam	Terganggunya operasional SIMRS	1
3	SIM-RS	< 12 jam	Gagalnya proses bisnis pada unit-unit yang ada di RSUD Arifin Achmad yang menggunakan SIMS	3

2.4.4 Identifikasi Level Risiko

Pada tahapan ini, penilaian terhadap *level* risiko melibatkan dua bagian, yaitu penilaian berdasarkan *level* probabilitas terjadinya ancaman dan kelemahan serta *level* dampak dari risiko yang muncul terhadap jalannya bisnis organisasi. Untuk mempermudah proses identifikasi *level* risiko aset dapat menggunakan matriks *level* risko dibawah ini.

Tabel 2. 8 Matriks *level* risiko (Utomo et al., 2012)

Probalitas Ancaman	**Dampak Bisnis**				
	Not Critical (0)	**Minor Critical** (1)	**Mayor Critical** (2)	***High* Critical** (3)	**Very *High* Critical** (4)
Low (0.1)	***Low*** 0	***Low*** 0.1	***Low*** 0.2	***Low*** 0.3	***Low*** 0.4
Medium (0.5)	***Low*** 0	***Medium*** 0.5	***Medium*** 1	***Medium*** 1.5	***Medium*** 2
High (1.0)	***Low*** 0	***Medium*** 1	***Medium*** 2	***High*** 3	***High*** 4

Untuk menentukan status dari aset yang sudah teridentifikasi nilai risikonya diterima atau perlu dilakukan pengelolaan terhadap risiko tersebut, maka perlu

diketahui nilai dari risiko aset tersebut. Nilai risiko aset dihitung dengan menggunakan persamaan rumus:

Nilai Risiko (NR) = N Aset x BIA x N Ancaman (NT)

Berikut ini contoh dari perhitungan nilai risiko yang dapat dilihat pada tabel 2.9:

Tabel 2. 9 Nilai risiko aset

No	Aset SI/TI	Nilai Aset (NA)	Nilai Ancaman dan Kelemahan (NT)	Nilai BIA	Nilai Risiko NAxNTxBIA
1	Informasi MOU	8	0.0429	4	1.3728
2	Server	7	0.0429	1	0.3003
3	SIM-RS	8	0.0429	3	1.0296

Tabel 2. 10 Level risiko aset

No	Aset SI/TI	Nilai Risiko	Level Risiko
1	Informasi MOU	1.544	*Medium Risk*
2	Server	0.3003	*Low Risk*
3	SIM-RS	3.0296	*High Risk*

2.4.5 Identifikasi dan Evaluasi Penanganan Risiko

Menurut (Iffano & Riyanarto, 2009) setelah melakukan penilaian risiko dan mengetahui *level* risiko yang terdapat pada aset organisasi, langkah selanjutnya adalah menentukan bagaimana kriteria penerimaan risiko aset tersebut. Kriteria ini digunakan sebagai acuan tindakan apa yang dilakukan oleh organisasi terhadap aset yang memiliki nilai risiko kritis dan dampak yang ditimbulkan jika terjadi kegagalan keamanan informasi pada organisasi. Tujuan dari langkah ini adalah melakukan kegiatan identifkasi dan menentukan pilihan penanganan risiko jika risiko yang timbul tidak langsung diterima akan tetapi perlu dilakukan pengelolaan lebih lanjut dengan menggunakan kriteria penerimaan yang telah ditentukan. Berikut ini kriteria penerimaan risiko dapat dikategorikan sebagai berikut:

1. Risiko diterima (*Risk acceptance*)

   Menerima risiko dengan menerapkan kontrol keamanan yang sesuai**.**

2. Risiko direduksi (*Risk reduction*)

   Menerima risiko yang terjadi direduksi dengan menggunakan Kontrol Keamanan sampai pada *level* yang dapat diterima oleh organisasi.

3. Risiko dialihkan (*Risk transfer*)

   Menerima risiko dengan mentransfer risiko kepada pihak ketiga (Asuransi, *vendor*, *supplier*, atau pihak tertentu) untuk penanganan dan mengurangi dampak yang ditimbulkan.

2.5 Standar dan Kerangka Kerja Keamanan Informasi

Keamanan informasi menjadi penting bagi organisasi saat ini, karena tidak hanya informasi internal organisasi saja yang harus dipertahankan, tetapi juga informasi pelanggan juga perlu dipertimbangkan (Aginsa et al., 2016), menurut Surat Edaran Menteri Komunikasi dan Informatika. No. 05/SE/M.KOMINFO/07/2001, tentang Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik maka setiap Penyelenggara Pelayanan Publik harus menerapkan Tata Kelola Keamanan Informasi secara andal dan aman serta bertanggung jawab sesuai dengan ketentuan Pasal 15 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Saat ini pada ruang lingkup keamanan informasi sudah banyak dikembangkan suatu standar dan kerangka kerja yang membantu *enterprise* atau organisasi dalam mengatur tingkat keamanan informasi yang dikelola serta prosedur keamanan informasi apa saja yang harus dilaksanakan. Berikut ini beberapa standar dan kerangka kerja yang digunakan dalam mngukur tingkat keamanan informasi:

1. *National Instite of Standards and Technology* (NIST) 800-30

   NIST 800-30 dipublikasikan pada tahun 2002 oleh *National Institute of Standards and Technology*. NIST 800-30 merupakan publikasi khusus mengenai *Risk Guide for Information Technology System*. NIST 800-30 menyediakan dasar dalam pengembangan program manajemen risiko yang berisi arahan atau pedoman yang dibutuhkan untuk menilai dan memitigasi risiko yang teridentifikasi didalam suatu teknologi informasi. Tujuan dari NIST 800-30

adalah untuk membantu organisasi dalam mengelola risiko terkait teknologi informasi dengan baik (NIST, 2002).

2. *Information Technology Insfrastructure Library* (ITIL)

   ITIL merupakan seperangkat konsep dan praktik yang menggambarkan *best practice* dalam mengelola layanan, pengembangan serta operasi teknologi Informasi. ITIL menyediakan kerangka kerja bagi tata kelola TI yang berfokus kepada pengukuran secara terus-menerus serta perbaikan kualitas layanan TI yang diberikan, baik dari sisi bisnis maupun dari sisi pelanggan (ItSMF, 2007).

3. *Control Objective for Information and Related Technology* (COBIT)

   COBIT merupakan standar yang dikeluarkan oleh IT Governance Institute (ITGI) pada tahun 1996. COBIT merupakan referensi kerangka kerja yang umum digunakan dalam pengimplementasian kontrol sebagai langkah mitigasi risiko terhadap setiap proses-proses TI yang diantaranya kesenjangan antara persyaratan kontrol, masalah teknis, risiko bisnis, dan masalah keamanan (ISACA, 2012).

4. ISO (*International Organization for Standardization*) dan IEC (*International Electrotechnical Commission*) 27001

   ISO/IEC 27001 merupakan dokumen standar Sistem Manajemen Keamanan Informasi (SMKI) atau *Information Security Management Systems* (ISMS) yang berisi panduan secara umum mengenai apa saja yang harus dilakukan dalam usaha pengimplementasian konsep-konsep keamanan informasi di organisasi. Kontrol keamanan berdasarkan ISO/IEC 27001 terdiri dari 11 klausul kontrol keamanan (*security control clauses*), 39 objektif kontrol (*control objectives*) dan 133 kontrol keamanan/ kontrol (*controls*).

Berikut ini penjelasan mengenai perbandingan antara standar dan kerangka kerja yang telah jelaskan diatas:

Tabel 2. 11 Perbandingan Standar dan Kerangka Kerja KeamananInformasi

Kriteria	NIST	ITIL	COBIT	ISO 27001
Ruang lingkup Standar keamanan informasi	√	Kerangka kerja	Kerangka kerja	√

		manajemen tingkat layanan TI	proses tata kelola TI	
Mendefinisikan persyaratan peningkatan berkelanjutan Sistem Manajemen Keamanan Informasi (SMKI).	√	-	-	√
Sertifikasi Manajemen Keamanan Informasi	-	-	-	√
Mengacu pada 3 Aspek Keamanan informasi (kerahasiaan, keutuhan dan ketersediaan)	-	-	-	√
Penilaian mengenai tingkat kematangan SMKI (*Maturity level*)	-	-	√	√

2.6 ISO 27001

ISO (*International Organization for Standardization*) dan IEC (*International Electrotechnical Commission*) membentuk suatu badan khusus untuk standarisasi beberapa aspek di seluruh dunia. badan nasional yang menjadi anggota ISO/IEC berpartisipasi dalam pengembangan Standar Internasional melalui komite teknis yang ditetapkan oleh organisasi masing-masing negara untuk menangani bidang-bidang tertentu kegiatan teknis, tidak terkecuali pada bidang keamanan informasi.

Keamanan informasi dicapai dengan menerapkan sebuah kontrol terintegrasi, mulai dari kebijakan, proses, prosedur, struktur organisasi, serta perangkat lunak dan perangkat keras. Sebuah Sistem Manajemen Keamanan Informasi (SMKI) adalah cara untuk melindungi dan mengelola informasi berdasarkan pendekatan risiko yang sistematis, untuk menetapkan, menerapkan, mengoperasikan, memantau, mengkaji, memelihara, dan meningkatkan keamanan informasi. ISO 27001 merupakan salah satu standar SMKI yang banyak diadopsi organisasi. Standar ini mengadopsi pendekatan proses model *Plan-Do-Check-Action* untuk penetapan, penerapan, pengoperasian, pemantauan, pengkajian, pemeliharaan dan perbaikan SMKI suatu organisasi. Menurut (Chang et al., 2013)

ISO 27001 dapat membantu kalangan enterprise dalam mengidentifikasi berbagai potensi risiko mengenai keamanan informasi di organisasi.

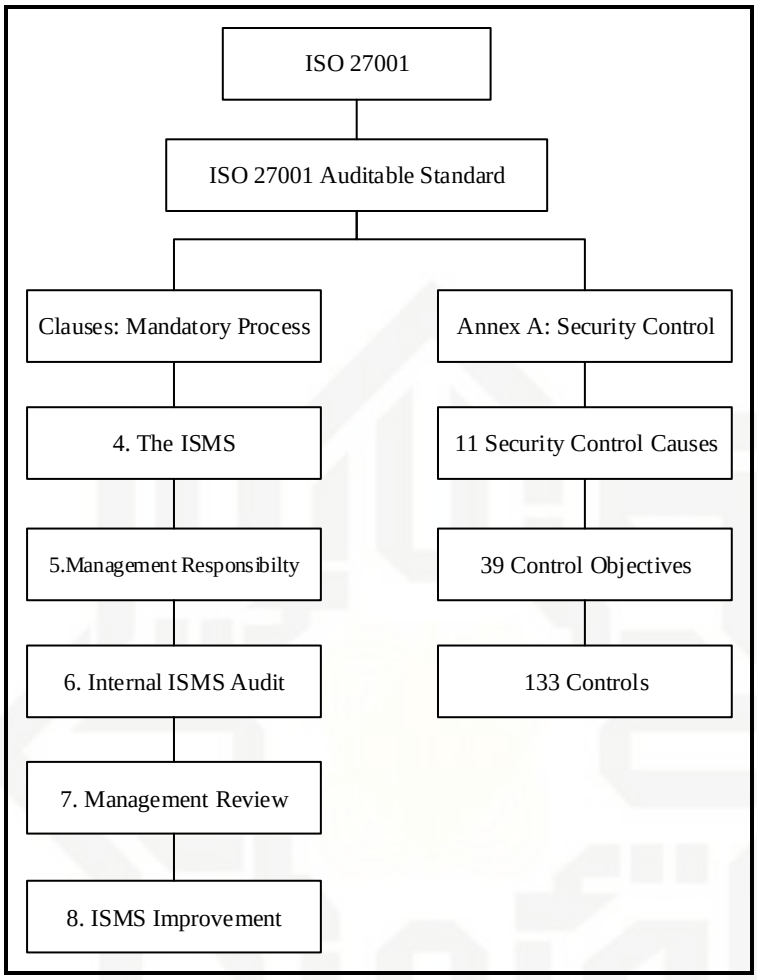
Struktur organisasi ISO 27001 dibagi dalam dua bagian besar yaitu :

1. Klausul *: Mandatory process*

   Klausul (pasal) berisi persyaratan atau kebutuhan dan ketentuan yang harus dipenuhi organisasi atau perusahaan dalam menerapkan SMKI dengan menggunakan standard ISO 27001.

2. Annex A : *Security Kontrol*

   Annex A adalah dokumen referensi yang disediakan dan dapat dijadikan rujukan untuk menentukan kontrol keamanan (*security* kontrol) yang ingin di implementasikan pada sistem manajemen keamanan informasi, Annex A ISO 27001 yang terdiri dari 11 klausul kontrol keamanan, 39 objektif kontrol dan 133 kontrol keamanan.



Gambar 2. 2 Struktur Organiasi ISO 27001 (Iffano & Riyanarto, 2009)

Berikut ini struktur isi dokumen ISO 27001:

No	Struktur Isi Dokumen	Klausul Terkait
1	Panduan Umum (General)	Klausul 1, 2, dan 3
2	Sistem Manajemen Keamanan Informasi	Klausul 4
3	Tanggung jawab manajemen (*Management Responsibilty*)	Klausul 5
4	Audit Internal SMKI (*Internal* ISMS *Audit*)	Klausul 6
5	Tinjauan manajemen SMKI (*Management review of the* ISMS)	Klausul 7
6	Perbaikan dan Pengembangan SMKI (ISMS *Improvement*)	Klausul 8
7	Kontrol keamanan SMKI	A.5 s/d A.15

Dalam buku "Sistem Manajemen Keamanan Informasi – Berbasis ISO 2001" karangan Sarno dan Iffano, Beberapa hal penting yang dapat dijadikan pertimbangan penggunaan standar ISO 27001 dipilih sebagai standar untuk implementasi SMKI suatu organisasi adalah sebagai berikut :

ISO 27001 telah menyediakan model lengkap terkait dengan bagaimana hal-hal berikut dilakukan. :

1. Membangun SMKI (*Establishing*)
2. Implementasi SMKI (*Implementing*)
3. Operasional SMKI (*Operating*)
4. Memonitor SMKI (*Monitoring*)
5. Mengkaji ulang SMKI (*Maintaining*)
6. Mengembangkan SMKI (*Improving*)

Dan juga ISO 27001 didesain agar pengimplementasian SMKI dengan standar ini menjadi lebih fleksibel penerapanya karena dapat disesuai dengan hal-hal berikut:

1. Kebutuhan organisasi (*Needs*)
2. Tujuan organisasi yang akan dicapai (*Objectives*)
3. Persyaratan keamanan yang diperlukan (*Security Requirement*)
4. Proses bisnis yang ada (*The Processes*)
5. Jumlah pegawai dan ukuran struktur organisasi (*Employee And The Size Of Organization*)

Sehingaa dengan menggunakan standar ISO 27001 dalam pengimplementasiannya dapat sangat tergantung dengan keadaan dan kebutuhan organisasi, karena organisasi yang proses bisnisnya sederhana akan membutuhkan SMKI yang sederhana pula. Didalam bukunya Sarno dan Iffano mengatakan kontrol keamanan berdasarkan ISO 27001 terdiri dari 11 klausul kontrol keamanan (*security control clauses*), 39 objektif kontrol (*control objectives*) dan 133 kontrol keamanan/kontrol (*controls*). Berikut ini rangkuman annex klausul keamanan yang terdapat pada ISO 27001.

Tabel 2. 12 Rangkuman annex klausul keamanan yang terdapat pada ISO 27001 (Iffano & Riyanarto, 2009)

No	No. Klausul		Jumlah	
			Objektif Kontrol	Kontrol
1	A.5	Kebijakan Keamanan Informasi	1	2
2	A.6	Organisasi Keamanan Informasi	2	11
3	A.7	Tanggung jawab terhadap aset	2	5
4	A.8	Keamanan sumber daya manusia	3	9
5	A.9	Keamanan fisik dan lingkungan	2	13
6	A.10	Manajemen komunikasi dan operasi	10	32
7	A.11	Kontrol Akses	7	25
8	A.12	Akuisisi Sistem Informasi, Pembangunan dan Pemeliharaan	6	16
9	A.13	Manajemen kejadian keamanan informasi	2	5
10	A.14	Manajemen kelangsungan bisnis *(Business Continuity Management)*	1	5
11	A.15	Kepatutan *(Compliance)*	3	10
Total: 11			**Total: 39**	**Total: 133**

ISO 27001 digunakan sebagai salah satu standar manajemen keamanan informasi yang memberikan gambaran secara umum mengenai apa saja yang harus dilakukan organisasi dalam usaha mereka mengimplementasikan konsep-konsep keamanan informasi di organisasi. Berikut *detail* penjelasan klausul keamanan yang terdapat pada ISO 27001 dijelaskan dalam tabel 2.12

Tabel 2. 13 Ringkasan klausul kontrol ISO 27001 (Iffano & Riyanarto, 2009)

No	No. Klausul	Klausul Kontrol Keamanan	Penjelasan
1	A.5	Kebijakan Keamanan Informasi	Memberikan arahan kepada manajemen organisasi dan dukungan

No	No. Klausul	Klausul Kontrol Keamanan	Penjelasan
			untuk keamanan informasi dalam hubungannya dengan persyaratan bisnis organisasi, hukum, dan aturan yang sedang berlaku.
2	A.6	Organisasi Keamanan Informasi	Bagaimana mengelola keamanan informasi di dalam organisasi baik itu yang hubungan internal organisasi maupun terhadap pihak eksternal (pihak eksternal, *vendor*, dll.)
3	A.7	Tanggung jawab terhadap aset	Kontrol yang terkait dengan inventarisasi aset dan penggunaan diterima, juga untuk klasifikasi informasi dan penanganan media
4	A.8	Keamanan sumber daya manusia	Kontrol terkait pengelolaan sumber daya manusia sebelum kerja, selama, dan setelah pekerjaan
5	A.9	Keamanan fisik dan lingkungan	Kontrol yang mendefinisikan daerah aman, kontrol masuk, perlindungan terhadap ancaman, keamanan peralatan, pembuangan aset-aset yang benar, serta kebijakan terhadap pengelolaan aset.
6	A.10	Manajemen komunikasi dan operasi	Untuk memastikan keamanan operasi dan mencegah terjadi kesalahan dalam mengoperasikan fasilitas-fasilitas pemrosesan informasi.Kontrol yang berkaitan dengan keamanan jaringan, layanan jaringan, transfer informasi, dll.
7	A.11	Kontrol Akses	Kontrol untuk kebijakan kontrol akses, manajemen akses pengguna, sistem dan kontrol akses aplikasi, dan tanggung jawab pengguna
8	A.12	Akuisisi Sistem Informasi, Pembangunan dan Pemeliharaan	Untuk memastikan bahwa keamanan adalah bagian dari sistem informasi yang ditinjau dari bagaimana data *input*an, kontrol dalam pemrosesan serta validasi data dari *output* yang dihasilkan.

No	No. Klausul	Klausul Kontrol Keamanan	Penjelasan
9	A.13	Manajemen kejadian keamanan informasi	Kontrol untuk melaporkan peristiwa dan kelemahan, mendefinisikan tanggung jawab, prosedur tanggap, dan pengumpulan bukti terkait kejadian yang mengancam keamanan dari informasi.
10	A.14	Manajemen kelangsungan bisnis *(Business Continuity Management)*	Untuk menghindari gangguan terhadap aktifitas bisnis serta untuk menjaga proses-proses bisnis yang kritis dari kegagalan dan dampak yang lebih besar atau bencana terhadap sistem informasi.
11	A.15	Kepatutan *(Compliance)*	Kontrol yang memerlukan identifikasi hukum dan peraturan yang berlaku, perlindungan kekayaan intelektual, perlindungan data pribadi, dan ulasan keamanan informasi.

2.7 Uji Kematangan (*Maturity Level*)

Menurut (Iffano & Riyanarto, 2009) model tingkat kematangan SMKI pada sebuah organisasi akan menentukan tingkat manfaat dan bagaimana kesesuaian SMKI yang telah diterapkan dikaitkan dengan yang diharapkan dan disesuaikan dengan standar yang ada yaitu ISO 27001.

Model tingkat kematangan SMKI yang digunakan dalam penelitian ini menggunakan model yang yang mengacu pada tingkat kematangan kerangka kerja CMMI (*Capability Maturity Model Integration*). Pada jurnal *Assesing IT Security Governance Trough a Maturity Model and the Definition of a Governance Profile* oleh Jean dan Carbonel dalam penelitian (Komalasari & Perdana, 2009), CMMI adalah model pengukuran tingkat kematangan yang dapat digunakan untuk melakukan penilaian manajemen IT dengan lebih efisien dan dapat diterapkan ke masing-masing klausul yang ada pada ISO 27001.

Tabel 2. 14 Model Kematangan Generik (IT Governance Institute, 2007)

No	Tingkatan Kematangan	Keterangan	Definisi
1	0 (*Non Existent*) (0 – 0.49)	Pasif	Organisasi tidak mengetahui bahwa terdapat permasalahan yang harus diatasi.
2	1 (*Initial*) (0.50 – 1.49)	Reaktif	Mulai adanya pemahaman bahwa organisasi mengetahui adanya permasalahan yang harus diatasi. Kelemahan-kelemahan yang bersifat teknis dan non-teknis belum teridentifikasi dengan baik. Tingkat kesadaran tanggung jawab pihak yang terlibat masih rendah.
3	2 (*Repeatable*) (1.5 – 2.49)	Aktif	Upaya pengamanan sudah ada namun hanya diterapkan di area teknis, dan belum adanya keterkaitan dengan langkah strategis yang efektif. Tidak terdapat pelatihan formal, pengkomunikasian prosedur, standar, dan tanggung jawab diserahkan kepada masing-masing individu pada organisasi. Terdapat tingkat kepercayaan yang tinggi terhadap individu sehingga memungkinkan terjadi error sangat besar.
4	3 (*Defined*) (2.5 – 3.49)	Terdefinisi	Sistem manajemen keamanan informasi sudah memiliki acuan dan diterapkan secara konsisten dan terdokumentasi. Kerangka kerja atau prosedur yang ada sudah memenuhi standar yang berlaku namun dalam tingkatan yang minim namun sudah menformalkan praktek yang berjalan. Secara umum pihak-pihak yang terlibat sudah menyadari tanggung jawab masing-masing.
5	4 (*Managed*) (3.5 – 4.49)	Terkelola	Manajemen mengawasi dan mengukur kepatutan terhadap prosedur dan mengambil tindakan jika proses tidak dapat dikerjakan secara efektif. Insiden diselesaikan melalui proses formal.

No	Tingkatan Kematangan	Keterangan	Definisi
			Kelemahan dalam SMKI teridentifikasi dengan baik dan secara konsisten dievaluasi dan ditindaklanjuti.
6	5 (*Optimized*) (4.5 – 5.00)	Optimal	Proses diterapkan secara menyeluruh, berkelanjutan dan efektif dengan bakuan yang sesuai dengan pengelolaan terstruktur, Proses telah dipilih ke dalam tingkat praktek yang baik, Teknologi informasi digunakan secara terpadu untuk mengotomatisasi alur kerja, penyediaan alat dan sarana untuk peningkatan kualitas dan efektivitas kontrol membuat organisasi cepat beradaptasi. SMKI diterapkan secara menyeluruh, berkelanjutan dan efektif dengan bakuan yang sesuai dengan pengelolaan terstruktur.

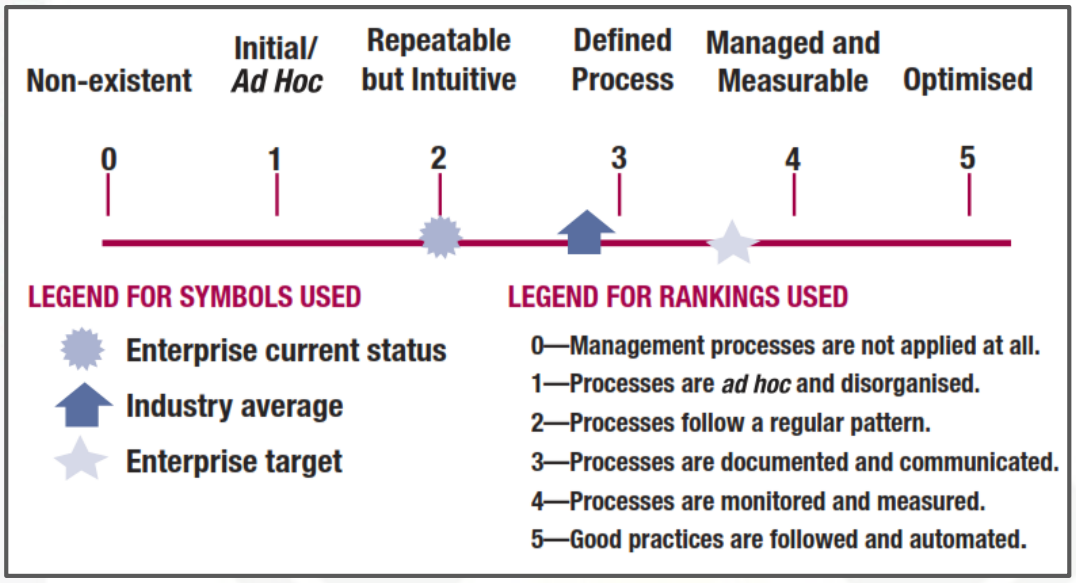
Menurut (IT Governance Institute, 2007) analisis model kematangan (*maturity level*) dapat digunakan untuk mengidentifikasi status industri saat ini, target dan kondisi yang di inginkan perusahaan dalam hal peningkatan kualitas layanan, dan pertumbuhan yang di inginkan antara *as-is* (saat ini) dan *to-be* (masa mendatang). Pada penelitian ini, target *maturity level* dimasa mendatang RSUD Arifin Achmad di identifikasi berdasarkan beberapa faktor yang diantaranya:

1. Visi dan Misi RSUD Arifin Achmad.
2. Dokumen *IT Master Plan* 2017-2019

Berdasarkan faktor-faktor tersebut, maka untuk rentang antara tahun 2017-2019 (jangka pendek) dapat ditentukan bahwa tingkat kematangan yang diharapkan (*to-be*) organiasi adalah pada tingkatan 4 (*Managed*). Alasan tingkat kematangan yang yang diharapkan pada *level* atau indeks 4 (*Managed*) adalah berdasarkan hasil wawancara yang dilakukan (Lihat lampiran B) fokus manajemen EDP pada tahun 2017-2018 masih pada pembenahan fungsional SIMRS yang lama karena beberapa sistem SIMRS tidak sesuai dengan proses bisnis yang ada serta tampilannya yang menyulitkan *user* sehingga alokasi dana untuk pengembangan SI/TI secara merata dan keseluruhan menjadi terbatas namun komitmen manajemen terhadap

pengelolaan SI/TI kearah yang lebih baik sudah ditunjukan dengan adanya perancangan *IT Master Plan* dan projek kerja pembenahan SIMRS.

Urutan tingkat kematangan tata kelola TI dalam perusahaan ditunjukkan pada Gambar dibawah ini:



Gambar 2. 3 Grafik representasi tingkat kematangan *(IT Governance Institute*, 2007)

Analisis pengukuran tingkat kematangan dilakukan berdasarkan celah yang ada antara target yang di inginkan dengan nilai yang saat ini dicapai oleh organisasi. Hal ini diharapkan dapat mengidentifikasi apa saja yang dibutuhkan oleh ketika ingin meningkatkan pengelolaan SI/TInya yang dalam hal ini pada aspek keamanan informasi sampai dapat mencapai target yang di inginkan.

2.8 Tinjauan Pustaka

Berikut ini rangkuman penelitian berdasarkan *literature review* jurnal yang berkaitan dengan *assessment* atau penilaian keamanan informasi dan langkah-langkah memanajemen keamanan informasi menggunakan standar analisis berbasis ISO 27001 dapat dilihat pada tabel 2.14 berikut:

Tabel 2. 15 Rangkuman penelitian terkait

No	Peneliti	Topik	Tahun	Masalah	Metode Penelitian	Metode Analisis Risiko	Hasil
1	(She-I Chang, Jung-Jei Su, Hsing-Jung Li) Sumber: *2013 IEEE 16th International Conference on Computational Science and Engineering*	*risk assessment Mechanism for Personal Information Operations – Case Study by Hospital* Penilaian keamanan informasi rumah sakit	**2013**	Sebagian besar masalah keamanan informasi dikarenakan kelemahan dari perangkat lunak dan perangkat keras dalam menjaga kerahasiaan informasi pribadi di rumah sakit.	Observasi Lapangan, Wawancara, dan Kuisioner.	ISO 27001	Dari penelitian yang dilakukan menghasilkan 64 faktor risiko yang dihasilkan dari 11 control ISO 27001.

No	Peneliti	Topik	Tahun	Masalah	Metode Penelitian	Metode Analisis Risiko	Hasil
2	(Michele Bava, Domenico Cacciari, Edoardo Sossa, Riccardo Zangrando) Sumber: *First International Conference on Computational Intelligence, Communication Systems and Networks*	*Information Security risk assessment in Healthcare: the Experience of an Italian Paediatric Hospital* Analisis risiko keamanan informasi *Italian Paediatric Hospital*	**2009**	Dengan penerapan *Health Information System* (HIS), muncul kekhawatiran akan risiko dan ancaman terkait keamanan informasi rumah sakit, serta kurangnya kesadaran mengenai masalah keamanan IT.	Observasi Lapangan, dan Wawancara.	ISO 27001.	Keamanan TI adalah masalah teknologi, organisasi, dan pengelolaan SDM. Dari penelitian yang dilakukan menghasilkan 5 bagian kerentaan berdasarkan ISO 27001 yaitu: Logical (Mengenai masalah SOP), Infrastructural (Mengenai keamanan perangkat), Concerning Services (Mengenai pengelolaan aset), Organizational (Mengenai keadaan organisasi).
3	(Margo Utomo, dkk) Sumber:	Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses	**2012**	Bagaimana mengidentifikasi dan menganalisis risiko keamanan informasi yang berhubungan dengan akses kontrol	Observasi Lapangan, dan Wawancara.	ISO 27001	Berdasarkan analisis yang dilakukan menggunakan IS0 27001 pada klausul kontrol akses berhasil mengidentifikasi dua

No	Peneliti	Topik	Tahun	Masalah	Metode Penelitian	Metode Analisis Risiko	Hasil
	Jurnal Teknik Its Vol. 1, No. 1, (Sept. 2012) ISSN: 2301-9271	Berbasis ISO/IEC 27001:2005 Pada Kantor Pelayanan Perbendaharaan Surabaya I		yang terdapat di KPPN Surabaya I.			aset yang perlu dilakukan pengelolaan risikonya karena memiliki nilai risiko yang tinggi, yaitu Sistem operasi dan data *user/password*
4	Rizki Komalasari dan Ilham Perdana Sumber: Universitas Telkom Jurnal Sistem Informasi, Vol. 9 No. 2, September 2014: 201 - 216	Audit Keamanan Informasi Bagian Teknologi Informasi PT PLN (Persero) DJBB Menggunakan SNI ISO/IEC 27001.	**2014**	Terdapat beberapa permasalahan yang berpotensi mengancam keamanan informasi yang ada di PT. PLN yang ditemukan di beberapa aspek seperti pada aspek kebijakan, lingkungan, dan manajemen.	Observasi Lapangan, Wawancara, dan Lembar kerja audit.	ISO 27001.	Berdasarkan audit yang dilakukan menghasilkan temuan: Klausul kebijakan keamanan, keamanan fisik dan lingkungan berada pada *level* 4 (terkendali), klausul manajemen komunikasi dan operasi pada *level* 5 (optimal).

No	Peneliti	Topik	Tahun	Masalah	Metode Penelitian	Metode Analisis Risiko	Hasil
5	Abdul Hakim, dkk. Sumber: *Journal of Information Systems*, Volume 10, Issue 2, October 2014 dx.doi.org/10.21609/jsi.v10i2	Evaluasi Tata Kelola Teknologi Informasi Dengan Framwork Cobit. 5 di Kementerian ESDM.	**2014**	Permasalahan yang ada adalah belum adanya suatu sistem tata kelola terstandar baik dalam pengelolaan dan pengadaan perangkat TI pada setiap unit kerja Kementerian ESDM.	Observasi Lapangan, dan Wawancara.-	COBIT 5	Hasil tingkat model *capability* skala penelitian penerapan *framework* cobit 5 pada evaluasi tata kelola teknologi informasi di KESDM yaitu skala target 3 (*established process*) yang dapat ditarik kesimpulan bahwa perlu dilakukan pengoptimalan implementasi dan pemeliharaan TI dalam menunjang kinerja organisasi.
6	Fine Ermana, dkk. Sumber: Jurnal Sistem Informasi dan Komputer	Audit Keamanan Sistem Informasi Berdasarkan Standar ISO 27001 Pada	**2012**	Belum memiliki prosedur keamanan informasi pada area bisnis, sehingga diperlukan audit keamanan informasi untuk melihat seperti apa keadaan kontrol	Observasi Lapangan, Wawancara, dan Lembar kerja audit.	ISO 27001	Hasil *maturity level* didapat dari seluruh kontrol keamanan mendapatkan nilai sebesar 2,90 yang berarti bahwa kontrol keamanan masih berada pada *level* 2 *planned and tracked*

No	Peneliti	Topik	Tahun	Masalah	Metode Penelitian	Metode Analisis Risiko	Hasil
	Akuntansi: 2012	Pt. BPR Jatim.		keamanan informasinya.			(direncanakan dan dilacak) namun telah mendekati *level* 3 *well defined* (didefinisikan dengan baik) yang merupakan *level* yang diharapkan oleh organisasi.
7	Rosmiati dan Imam Riadi	Analisis Keamanan Informasi Berdasarkan Kebutuhan Teknikal Dan Operasional Mengkombinasikan Standar ISO 27001:2005 dengan *Maturity level* (Studi Kasus Kantor Biro Teknologi	**2016**	Sebagian besar proses pengelolaan adminsistrasi di organisasi telah menggunakan sistem elektronik yang menyimpan begitu besar informasi secara digital untuk itu organisasi harus menerapkan kebijakan yang tepat untuk melindungi aset informasi yang dimiliki dan melihat sejauh mana tingkat	Observasi Lapangan, Wawancara.	ISO 27001	Tingkat kematangan atau *maturity level* pada PT. XYZ rata-rata berada tingkat ke-2 (Repeatable but Intituitive) sehingga selanjutnya diperlukan perhatikan penting bagi *top* manajemen utk memperhatikan tingkat keamanan informasi PT. XYZ

No	Peneliti	Topik	Tahun	Masalah	Metode Penelitian	Metode Analisis Risiko	Hasil
		Informasi PT. XYZ)		kematangan SMKI organisasi.			
8	Adi Supriyatna Sumber: Prosiding Seminar Nasional Aplikasi Sains & Teknologi (SNAST) 2014 ISSN: 1979-911X	Analisis Tingkat Keamanan Informasi Akademik Dengan Mengkombinasikan Standar BS-7799 Dengan SSE-CMM	**2014**	Melihat seperti apa sistem keamanan pada sistem informasi akademik apakah sudah sesuai dengan standar atau tidak,dan mengukur Sejauh mana kesiapan sistem informasi akademik dalam penerapan standar keamanan informasi.	Observasi Lapangan, Wawancara, dan Kuesioner.	BS-7799	Penerapan standar keamanan informasi pada sistem informasi akademik berdasarkan BS-7799 masih belum siap karena dari 11 klausul yang ditetapkan, hanya tiga klausul saja yang baru memenuhi standar tingkat kematangan yaitu klausul kontrol akses, pengembangan sistem dan pemeliharaan dan klausul manajemen komunikasi dan operasi.
9	Titus Kristanto Sumber:	Perancangan Audit Keamanan Informasi Berdasarkan Standar ISO	**2014**	Bagaimana menganalisis risiko keamanan informasi yang mungkin terjadi pada PT. PT	Observasi Lapangan, Wawancara, dan Lembar kerja audit.	ISO 27001	Berdasarkan hasil temuan audit saat ini sistem manajemen keamanan informasi yang ada berada pada *level* 2 yaitu Repeatable

No	Peneliti	Topik	Tahun	Masalah	Metode Penelitian	Metode Analisis Risiko	Hasil
	Seminar Nasional Sistem Informasi Indonesia, 22 September 2014	27001 (Studi Kasus: PT Adira Dinamika Multi Finance)		Adira Dinamika Multi Finance.			but Intuitive atau Upaya pengamanan sudah ada namun hanya diterapkan di area teknis, dan belum adanya keterkaitan dengan langkah strategis yang efektif.

Perbedaan dan persamaan penelitian yang dilakukan terdahulu akan dijelaskan pada Tabel 2.15 berikut ini:

Tabel 2. 16 Persamaan dan Perbedaan Penelitian yang dilakukan

No	Peneliti	Topik	Persamaan Penelitian	Perbedaan Penelitian
1	(She-I Chang, Jung-Jei Su, Hsing-Jung Li)	*Risk assessment Mechanism for Personal Information Operations – Case Study by Hospital*.	1. Objek penelitian yang dipilih sama yaitu : Rumah sakit. 2.Metode analisis keamanan informasi sama, yaitu: ISO 27001.	1. Penelitian She-I Chang, dkk. tidak melakukan perhitungan *assessment checklist* sehingga tingkat *maturity level* penerapan SMKI tidak diketahui. 2. Penelitian She-I Chang, dkk. tidak melakukan identifikasi risiko pada aset SI/TI studi kasus.

No	Peneliti	Topik	Persamaan Penelitian	Perbedaan Penelitian
2	(Michele Bava, Domenico Cacciari, Edoardo Sossa, Riccardo Zangrando)	*Information Security risk assessment in Healthcare: the Experience of an Italian Paediatric Hospital*.	1.Objek penelitian yang dipilih sama yaitu : Rumah sakit. 2.Metode analisis keamanan informasi sama, yaitu: ISO 27001. 3.Juga melakukan identifikasi risiko pada aset TI instansi/organisasi.	1. Penelitian Bava, dkk. tidak melakukan perhitungan *assessment checklist* sehingga tingkat *maturity level* penerapan SMKI tidak diketahui.
3	(Margo Utomo, dkk)	Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis ISO/IEC 27001:2005 Pada Kantor Pelayanan Perbendaharaan Surabaya I.	1.Metode analisis keamanan informasi sama, yaitu: ISO 27001. 2.Juga melakukan identifikasi risiko pada aset TI instansi/organisasi.	1. Studi kasus penelitian. 2. Penelitian Margo, dkk. tidak melakukan perhitungan *assessment checklist* sehingga tingkat *maturity level* penerapan SMKI tidak diketahui.
4	Rizki Komalasari dan Ilham Perdana	Audit Keamanan Informasi Bagian Teknologi Informasi PT PLN (Persero) DJBB Menggunakan SNI ISO/IEC 27001.	1.Metode analisis keamanan informasi sama, yaitu: ISO 27001. 2.Juga melakukan perhitungan *maturity level*.	1. Penelitian Komalasari, dkk. tidak melakukan identifikasi risiko pada aset TI organisasi. 2. Studi kasus penelitian.
5	Abdul Hakim, dkk.	Evaluasi Tata Kelola Teknologi Informasi Dengan	1. Sama-sama melakukan audit pada TI	1. Perbedaan cakupan audit tata kelola operasional Tinya. Tentu

No	Peneliti	Topik	Persamaan Penelitian	Perbedaan Penelitian
		Framework Cobit. 5 di Kementerian ESDM.	2.Juga melakukan perhitungan *maturity level* untuk melihat sejauh apa penerapan teknologi informasinya.	beda pula metode analisis perencanaanya.
6	Fine Ermana, dkk.	Audit Keamanan Sistem Informasi Berdasarkan Standar ISO 27001 Pada PT. BPR Jatim	1.Metode analisis keamanan informasi sama, yaitu: ISO 27001. 2.Juga melakukan perhitungan *maturity level*.	1.Penelitian Ermana, dkk. tidak melakukan identifikasi risiko pada aset TI instansi/organisasi. 2. Studi kasus penelitian.
7	Rosmiati dan Imam Riadi	Analisis Keamanan Informasi Berdasarkan Kebutuhan Teknikal Dan Operasional Mengkombinasikan Standar ISO 27001:2005 dengan *Maturity level* (Studi Kasus Kantor Biro Teknologi Informasi PT. XYZ).	1.Metode analisis keamanan informasi sama, yaitu: ISO 27001. 2.Juga melakukan perhitungan *maturity level*.	1.Penelitian Rosmiati, dkk. tidak melakukan identifikasi risiko pada aset TI instansi/organisasi. 2. Studi kasus penelitian.
8	Adi Supriyatna	Analisis Tingkat Keamanan Informasi Akademik Dengan Mengkombinasikan Standar BS-7799 Dengan SSE-CMM.	1.Sama-sama melakukan perhitungan *maturity level* untuk melihat sejauh apa penerapan teknologi informasinya. 2.Cakupan audit tata kelola operasional TI-nya sama yaitu	1.Penelitian Adi, dkk. tidak melakukan identifikasi risiko pada aset TI instansi/organisasi. 2.Metode analisi keamanan informasinya berbeda. 3. Studi kasus penelitian.

No	Peneliti	Topik	Persamaan Penelitian	Perbedaan Penelitian
			berfokus pada manajemen keamanan informasi.	